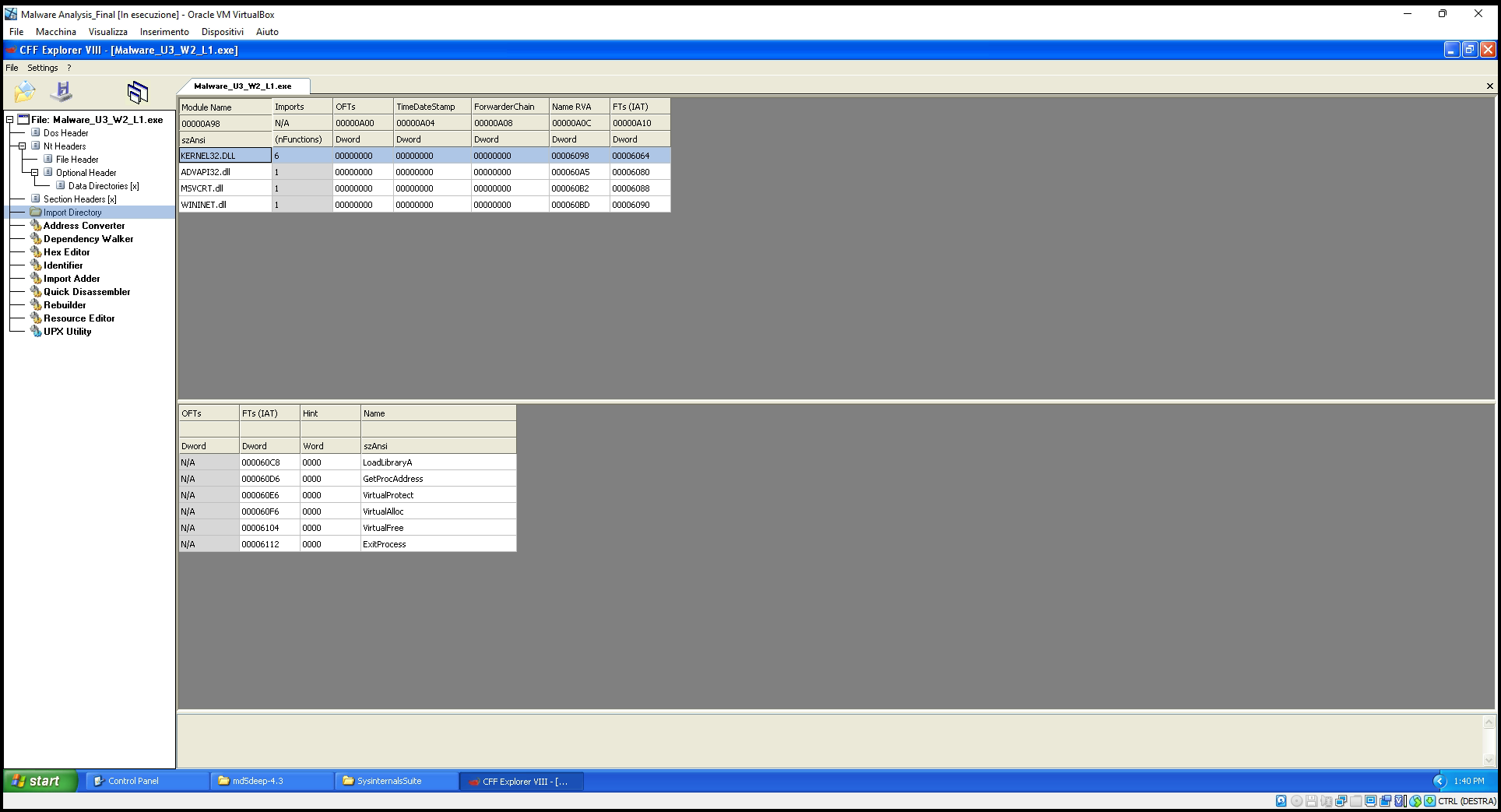
REPORT ANALISI MALWARE

Nel seguente report verranno mostrati le funzioni del malware in seguito alla sua disassemblazione.

Come programma è stato usato CFF EXPLORER, che permette l’uso di diversi tool in grado di poter analizzare nel dettaglio i malware.



Nel seguente screenshot sono elencate le seguenti librerie e funzioni:

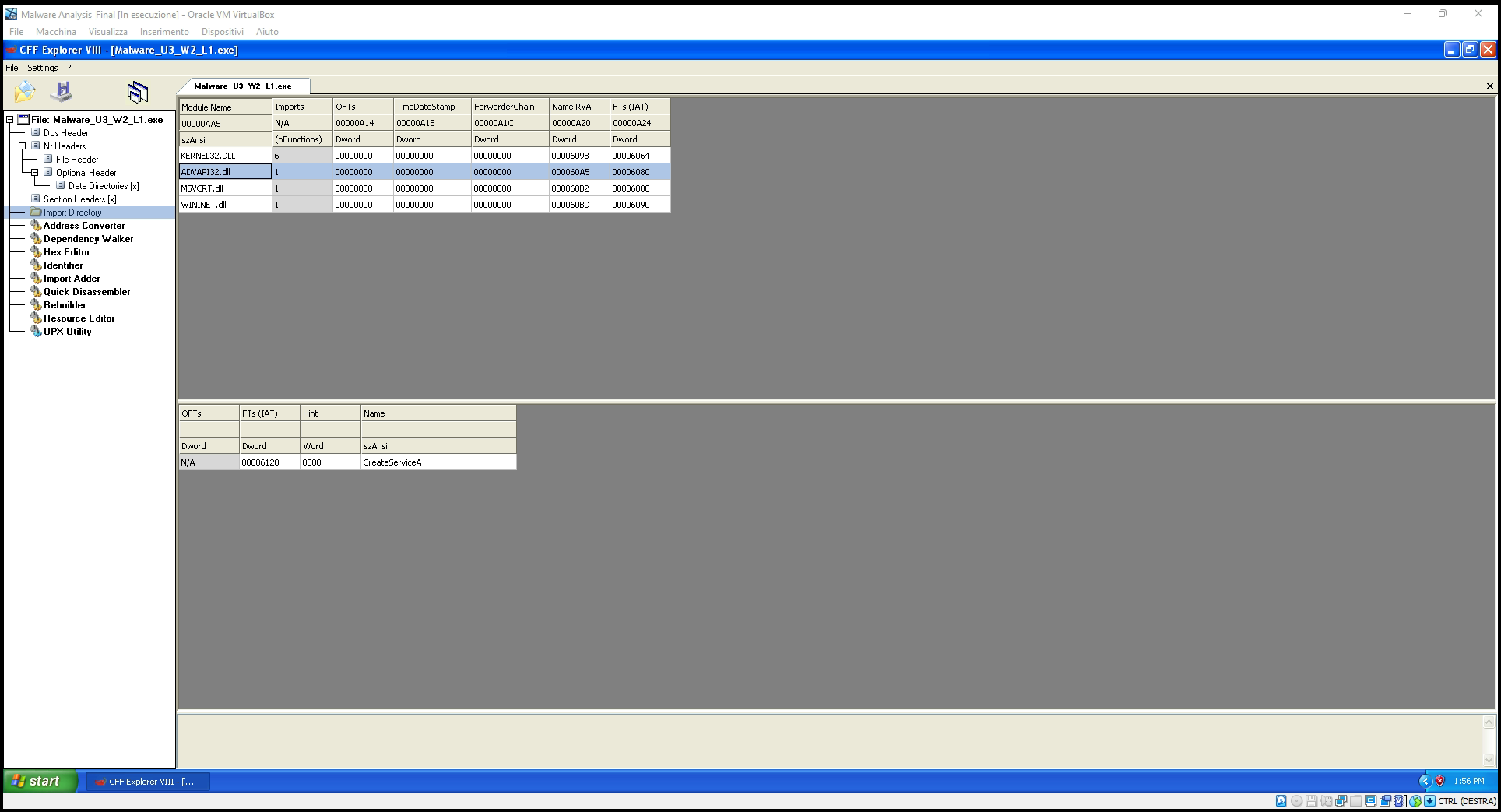
-Kernel32.dll; Contiene le funzioni principali per interagire con il sistema operativo ovvero manipolazione dei file e gestione della memoria.

Tali funzioni sono:

1. LoadLibraryA: Carica la libreria attuale
2. GetProcAddress: Repereisce l’indirizzo del processo di una funzione o di una variabile
3. VirtualProtect: Modifica i criteri di protezione
4. . VirtualAlloc: Gestisce l’allocamento della memoria virtuale

5. VirtualFree: Libera la memoria Virtuale

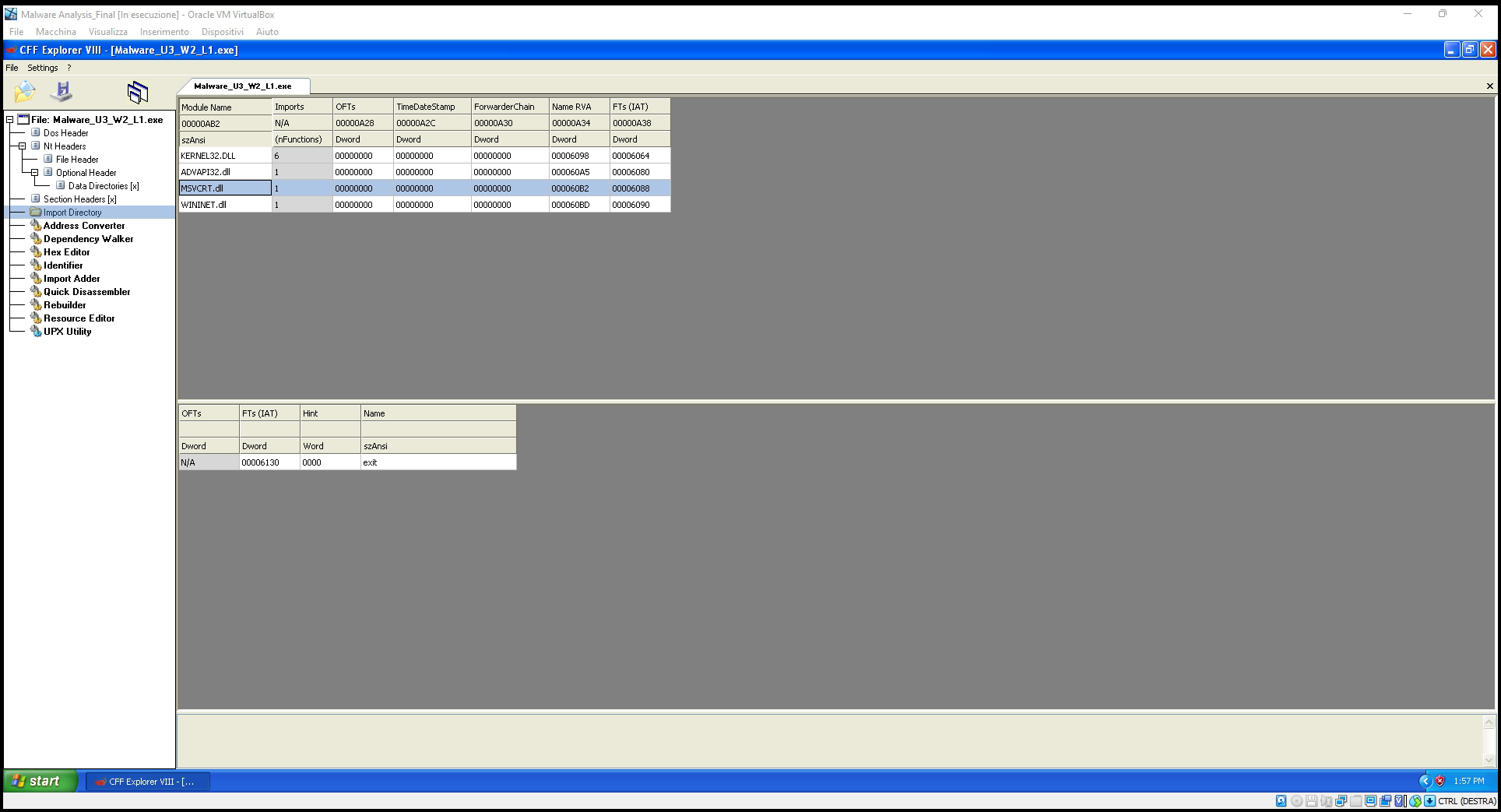
6. ExitProcess: chiude il processo



-Advapi32.dll; contiene le funzioni di per interagire con i servizi e sistema operativo Microsoft

Le sue funzioni sono:

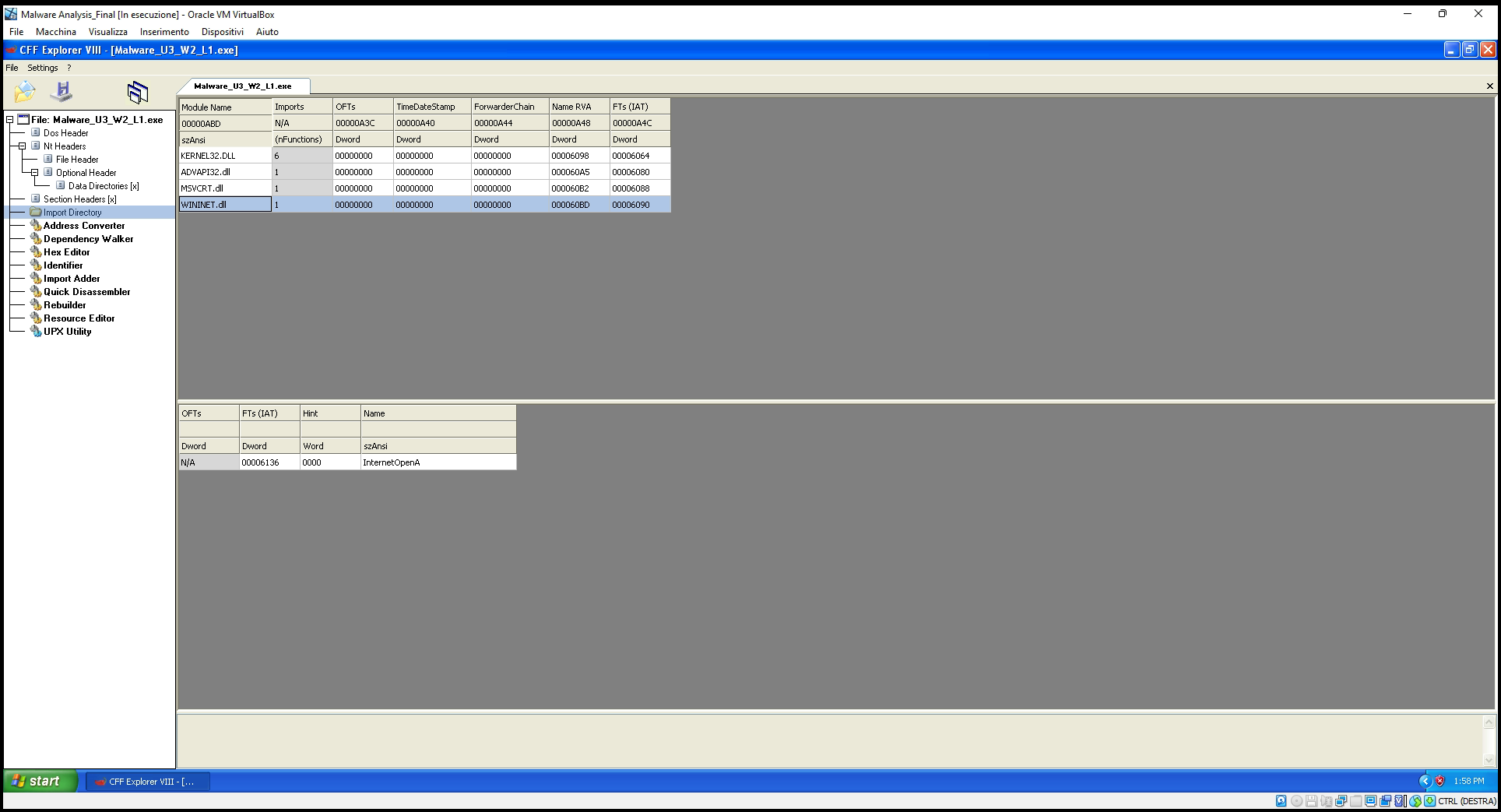
CreateServiceA:Crea il servizio su cui operare



-MSVCRT.dll: contiene funzioni per la manipolazione delle stringhe, allocazioni di memoria e altro come chiamate per input/output in stile linguaggio C

La sua funzione è

Exit: terminare il processo

Wininet.dll: Contiene funzioni per l’implementazione di alcuni protocolli come http,ftp,ntp.

Il suo servizio è InternetOpenA: stabilisce una connessione ad internet

Stabilite le seguenti analisi sul funzionamento del malware, si suppone che la minaccia in questione sia una backdoor, dato che stabilisce una connessione internet e modifica i criteri di sicurezza della macchina vittima.